REMARKS

Claims 1-14 are pending in the application. Claims 1-3, 5, 6, 8-10, 12, and 13 have been amended herein. Claims 4, 7, 11, and 14 have been canceled. Claims 15 and 16 have been added. Favorable reconsideration of the application, as amended, is respectfully requested.

I. REJECTION OF CLAIMS UNDER 35 USC § 102

Claims 1, 2, 5, 8, 9, and 12 stand rejected under 35 USC 102(e) based on being anticipated by US Patent 6,360,265 to Falck et al.

General Field of Applicants Invention

In general, the system (34) of the presently claimed invention facilitates the exchange of UDP media session datagrams with a client (such as a caller client 16) that is located on a private network (24) and served by a network address translation (NAT) proxy or firewall (28).

The system (34) includes a directory server (38) which maintains an open signaling channel that can be reverse translated by the NAT serving the caller client. The open signaling channel is initially identified by extracting the source IP address and source port number from a registration message initiated by the client and sent to the directory server through the NAT. A sequence of periodic ping messages initiated by the client and sent to the directory server though the NAT are used to maintain the open signaling channel through the NAT. (See P10, L4-L15, Figures 4a and 4b, and P14, L13-P15, L24).

When the caller client initiates a media session, it sends a call request message, or signaling message, to the directory server (Figure 2a, Signal 60 and Figure 5b, step 150). The directory server provides a real time protocol (RTP) channel of a call control manager (defined as a globally unique network address of the call control manager and a port number established by the call control manager for the session – see P17, L8-10) on the open channel (Figure 2a, signal 74 and Figure 5b, step 166).

The caller client then initiates the real time media stream of UDP datagrams to the RTP channel of the call control manager through the NAT (Figure 2a, signal 76 and Figure 7, step 240). The call control manager extracts a source IP address and a source port from the UDP datagram to identify an open media channel to the client that can be reverse translated by the NAT serving the client (Figure 7, steps 242-248). Datagrams from another client (such as the callee) are relayed to the caller client on the open media channel (Figure 2a, signals 80 and 82, Figure 7, steps 252 and 262).

Falck et al.

US Patent 6,360,265 to Falck et al. teaches a specialized NAT device that operates in place of a traditional NAT server. The NAT device of Falck et al. intercouples between the Internet and the local area network and performs network address translation (NAT) functions of IP layer translation between frames address on the local area network and frames address on the Internet.

By operating as a specialized NAT, the system of Falck et al. eliminates need for, and does not teach, a directory server maintaining an open signaling channel to a client served by a NAT wherein the open signaling channel is identified by extracting the source IP address and source port number of a registration and/or ping message initiated by the client.

Although the examiner refers to items 410, 420 and 430 of Figure 2 as a *"method for extracting source network address and a source port number form a datagram originated by a client"* step 410 refers to a device outside of the NAT (e.g. on the public network) sending an unsolicited inbound SYN message (e.g. this is the first message to establish a TCP/IP connection to the specialized NAT requesting a service on a well known port (C5, L57-58). The SYN message is not in response to an outbound message and is not being sent inbound on a channel extracted from an outbound message. The specialized NAT can not, and does not, reverse translate the SYN message in a traditional manner. Instead, at step 420 the specialized NAT recognizes that the message is to a well known port and

applies specialized rules for routing the inbound message to one of a plurality of servers (on the private network) that is able to handle the service request (see discussion C5, L55-C6, L17). Step 430 represents one of the specialized rules which includes the NAT substituting its own IP address.

Falck et al. does not teach a directory server providing, to the client on the open channel, an RTP channel to a call control manager such that the client can initiate the real time media stream of UDP datagrams to such RTP channel through the NAT.

In Falck et al., all communication is between: i) the Terminal 105 (the device outside the NAT in Falck et al.) and the specialized NAT; or ii) between the server 110, 112, 114 (the device inside the NAT of Falck et al. and the specialized NAT 106.

Falck et al. does not teach a call control manager extracting a source IP address and port number from a UDP datagram to identify an open media channel through the NAT that can be reverse translated by the NAT serving the client.

Instead, Falck et al. teaches providing identification of a media channel (e.g. provides the IP address of the specialized NAT and a port number) to the Terminal 102. This eliminates need for extraction of an IP address and port number for identifying an open channel.

As such, the specialized NAT of Falck et al. does not perform inbound translation in the traditional NAT manner of looking up an outbound message to which the inbound message is a reply. Instead, inbound translation performed by Falck et al. is in accordance with the specialized translation rule (Figure 5) for a non-well-known port (e.g. the port number is not translated and the local destination IP address is determined based on the range within which the destination port exists).

Phomsopha

US Published Application 2003/0048780 to Phomsopha teaches source IP address and port extraction to identify a reverse channel through a NAT firewall for

a media session. In more detail, the device behind the firewall opens a traditional TCP/IP connection through the NAT firewall to an Internet server, obtains through the TCP/IP session a port number assigned by the Internet Server for the media session, and sends a UDP "priming packet" to the Server. The Server extracts the source IP address and port number from the priming packet to identify the reverse channel through the NAT.

The system taught by Phomsopha requires that the client have sufficient information to establish the initial TCP/IP connection to the Server to which the UDP media session is to be established. This enables the Server to identify its assigned port for the UDP session.

Phomsopha does not address how the client identifies the Server to which the UDP media session is to be established. The system of the applicant's invention addresses the unresolved problem of Phomsopha. The directory server of the applicant's invention performs unique steps for identifying, to the caller client, the IP address and port number assigned by the call control manager (The real time protocol channel) to which the caller client is to initiate the UDP media session.

Kennedy (included in IDS)

US Published Application 2004/0252683 to Kennedy teaches source IP address and port extraction. Kennedy teaches a system and method where the device behind a NAT (e.g. Client B for example) periodically sends frames to an application server 105. The application server extracts the IP address and port number to identify a channel for exchanging control messages with Client B.

When a media session is to be set up between Client B and another device (Client A for example), Client B sends a special message to a port number of the application server 105. The Application server 105 extracts the IP address and port number to identify an inbound channel to Client B. The application server 105

provides this extracted IP address and port number to Client A (through the control message channel with Client A).

It is then assumed that Client A can send data to Client B on such extracted channel. However, it must be noted that the teachings of Kennedy **WILL NOT WORK** in a situation wherein the NAT will reverse translate an inbound frame that is not a true "response frame" – meaning that the inbound frame (from client A) does not include the same source IP address and port number as destination IP address and port number (e.g. the application server 105) to which the special message was originally sent.

The applicants invention, on the other hand, teaches a unique system and method for identifying, to the caller client behind the NAT, the IP address and port number of the call control manager so that the caller client may initiate UDP frames of the media session the call control manager and the call control manager itself can perform the IP address and port extraction to identify a true reverse channel through the NAT to the caller client.

Claim 1

Claim 1, as amended, is directed to a device for sending media session datagrams representing real time streaming media frames to a caller client (16) independent of whether the caller client (16) is served by a network address proxy (28). The device comprises a directory server (38) and a call control manager (36).

The directory server (38) receives a registration request from the caller client (Figure 4a, step 190) and extracts a source network address and a source port number from the registration request to identify an open signaling channel to the caller client from the directory server that can be reverse translated by the NAT 28 (Figure 4a, step 194, P15, L7-L9).

With reference to Figure 2a as an example, the directory server further: i) receives a media session signaling message originated by the caller client (Figure 2a, signal 60 and Figure 5b, step 150); ii) obtains a real time protocol channel from

the call control manager (Figure 2a, signal 72 and Figure 5b, step 166); and iii) returns a response signal to the caller client on the open signaling channel (Figure 2a, signal 74). The response signal includes the real time protocol channel provided by the call control manager.

The call control manager: i) provides the real time protocol channel to the directory server (Figure 2a, signal 72 and Figure 6, steps 226 and 228); ii) receives a media session datagram from the caller client to the real time protocol channel (Figure 2a, signal 76 and Figure 7, step 240); iii) extracts a source network address and a source port number from the media session datagram to identify an open media channel to the caller client from the call control manager that can be reverse translated by the NAT (Figure 7, steps 242-248); and iv) relays media session datagrams received from a callee client to the caller client on the open media channel (Figure 2a, steps 80 and 82 and Figure 7, steps 252 and 262).

Claim 5

Claim 5, as amended, is directed to a device for sending media session datagrams representing real time streaming media frames to a caller client (16) independent of whether the caller client (16) is served by a network address proxy (28). The device comprises a directory server (38) and a call control manager (36).

The directory server receiving a registration request originated by the caller client and extracts a source network address and a source port number from the registration request.

If the extracted source network address matches a client network address of the registration request, the directory server determines that the caller client is not served by a network address translation firewall and recording such determination in a client database;

If the extracted source network address is different than a client network address of the registration request, the directory server determines that the caller client is served by a network address translation firewall and recording the extracted source network address and source port number in the client database;

Again with reference to Figure 2a, the directory server further: i) receives a media session signaling request originated by the caller client; and ii) returns a response signal to the caller client on the open signaling channel recorded in the client database.

The response signal includes: i) a real time protocol channel of a call control manager if the record in the client database indicates that the caller client is served by a network address translation firewall; and ii) a real time protocol channel of a callee client identified in the media session signaling request if the record in the client database indicates that the caller client is not served by a network address translation firewall.

The call control manager operates as discussed above.

Claims 8 and 12

Claims 8 and 12, as amended, are directed to a method for sending media session datagrams representing real time streaming frames to a caller client independent of whether the caller client is served by a network address proxy.

The method of claim 8 comprises operating a directory server and a call control manager substantially as describe with respect to Claim 1. The method of claim 12 comprises operating a directory server and a call control manager substantially as describe with respect to Claim 5.

As such, claims 8 and 12 can be distinguished over the art of record for at least the same reasons

Dependent Claims.

The dependent claims, including claims 2 and 9 and new claims 15 and 16, each depend from one of the independent claims 1, 5, 8, or 12 and can be distinguished over Falck et al. and the other art of record for at least the same reasons.

II. REJECTION OF CLAIMS UNDER 35 USC § 103

Claims 3, 4, 6, 7, 10, 11, 13, and 14 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 6,360,265 to Falck et al. in view of US Published Application 2003/0048780 to Phomsopha. Claims 4, 7, 11, and 14 have been canceled.

Claim 3

Claim 3, as amended, is directed to a device for sending media session datagrams representing real time streaming media frames to a caller client (16) independent of whether the caller client (16) is served by a network address proxy (28). The device comprises a directory server (38) and a call control manager (36).

The directory server periodically receiving a UDP datagram comprising a ping message from the caller client and updates an open signaling channel field in a client database to reflect a source network address and a source port number extracted from the UDP datagram.

Again with reference to Figure 2a as an example, the directory server further: i) receives a media session signaling message originated by the caller client (Figure 2a, signal 60 and Figure 5b, step 150); ii) receives identification of a real time protocol channel from the call control manager (Figure 2a, step 74 and Figure 5b, step 166); and iii) returns a response signal to the caller client on the open signaling channel (82).

The call control manager operates as discussed above.

Claim 6

Claim 6, as amended, is directed to a device for sending media session datagrams representing real time streaming media frames to a caller client (16) independent of whether the caller client (16) is served by a network address proxy (28). The device comprises a directory server (38) and a call control manager (36).

The directory server receives a registration request originated by the caller client and extracts a source network address and a source port number from the registration request.

If the extracted source network address matches a client network address of the registration request, the directory server determines that the caller client is not serviced by a network address translation firewall and recording such determination in a client database.

If the extracted source network address is different than a client network address of the registration request, the directory server determines that the caller client is served by a network address translation firewall and recording the extracted source network address and source port number in the client database as an open signaling channel to the caller client;

The directory server further: i) periodically receives a UDP datagram comprising a ping message from the caller client; and ii) updates the open signaling channel to the caller client in the client database to reflect a source network address and a source port number extracted from the UDP datagram.

The directory server further yet receives a media session signaling request originated by the caller client and returns a response signal to the caller client on the open signaling channel recorded in the client database.

The response signal includes: i) a real time protocol channel of a call control manager if the record in the client database indicates that the caller client is served by a network address translation firewall; and ii) a real time protocol channel of a callee client identified in the media session signaling request if the record in the client database indicates that the caller client is not served by a network address translation firewall.

The call control manager operates as discussed above.

Claims 10 and 13

Claims 10 and 13, as amended, comprise a method for sending media session datagrams representing real time streaming frames to a caller client independent of whether the caller client is served by a network address proxy.

The method of claim 10 comprises operating a directory server and a call control manager substantially as describe with respect to Claim 3. The method of

claim 13 comprises operating a directory server and a call control manager substantially as describe with respect to Claim 6.

As such, claims 10 and 13 can be distinguished over the art of record for at least the same reasons

III. CONCLUSION

Accordingly, claims 1-3, 5, 6, 8-10, 12, 13, 15, and 16 are believed to be allowable and the application is believed to be in condition for allowance. A prompt action to such end is earnestly solicited.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should a petition for an extension of time be necessary for the timely reply to the outstanding Office Action (or if such a petition has been made and an additional extension is necessary), petition is hereby made and the Commissioner is authorized to charge any fees (including additional claim fees) to Deposit Account No. 501825.

Respectfully submitted,

Timothy P. O'Hagan
Reg. No. 39,319

DATE: 3-15-06

Timothy P. O'Hagan
8710 Kilkenny Ct
Fort Myers, FL 33912
(239) 561-2300